1. Record Nr. UNINA9910797727603321

Autore	Johnson Leighton
Titolo	Security controls evaluation, testing and assessment handbook / / Leighton Johnson
Pubbl/distr/stampa	Amsterdam, Netherlands : , : Syngress, , 2016 ©2016
ISBN	0-12-802564-6 0-12-802324-4
Edizione	[1st edition]
Descrizione fisica	1 online resource (904 p.)
Disciplina	658.155
Soggetti	Risk management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover; Title Page; Copyright Page; Dedication; Contents; Introduction; Section I; Chapter 1 - Introduction to Assessments; Chapter 2 - Risk, Security, and Assurance; Risk management; Risk assessments; Security controls; Chapter 3 - Statutory and Regulatory GRC; Statutory requirements; Privacy Act - 1974; CFAA - 1986; ECPA - 1986; CSA - 1987; CCA - 1996; HIPAA - 1996; EEA - 1996; GISRA - 1998; USA PATRIOT Act - 2001; FISMA - 2002; Sarbanes-Oxley - 2002; Health Information Technology for Economic and Clinical Health Act - 2009; Executive Orders/Presidential Directives HIPAA Security RuleHIPAA Privacy Rule; HITECH Breach Reporting; OMB requirements for each agency; References; Chapter 4 - Federal RMF Requirements; Federal civilian agencies; DOD - DIACAP - RMF for DOD IT; IC - ICD 503; FedRAMP; NIST Cybersecurity Framework; References; Chapter 5 - Risk Management Framework; Step 1 - categorization; Step 2 - selection; Step 3 - implementation; Step 4 - assessment; Step 5 - authorization; Step 6 - monitoring; Continuous Monitoring for Current Systems; Chapter 6 - Roles and Responsibilities; Organizational roles; White House; Congress; OMB; NIST; CNSS; NSA NIAPDHS; DOD; Individual roles; System Owner; Authorizing Official; Information System Security Officer; Information System Security Engineer; Security Architect; Common Control Provider; Authorizing Official Designated Representative; Information Owner/Steward; Risk

Executive (Function); User Representative; Agency Head; Security Control Assessor; Senior Information Security Officer; Chief Information Officer; DOD roles; Section II ; Introduction; Chapter - 7 - Assessment Process; Focus; Guidance; SP 800-53A; RMF Step 4 - Assess Security Controls; SP 800-115; RMF Knowledge Service
ISO 27001/27002Chapter - 8 - Assessment Methods; Evaluation methods and their attributes; Processes; Interviews; Examinations; Observations; Document Reviews; Testing; Automated; Manual; Chapter - 9 - Assessment Techniques for Each Kind of Control; Security assessment plan developmental process; Security assessment actions; Security controls by family; Chapter - 10 - System and Network Assessments; 800-115 introduction; Assessment techniques; Network testing purpose and scope; ACL Reviews; System-Defined Reviews; Testing roles and responsibilities; Security testing techniques
Four phases of penetration testing

Sommario/riassunto

Security Controls Evaluation, Testing, and Assessment Handbook provides a current and well-developed approach to evaluation and testing of security controls to prove they are functioning correctly in today's IT systems. This handbook shows you how to evaluate, examine, and test installed security controls in the world of threats and potential breach actions surrounding all industries and systems. If a system is subject to external or internal threats and vulnerabilities - which most are - then this book will provide a useful handbook for how to evaluate the effectiveness of the security controls that are in place. Security Controls Evaluation, Testing, and Assessment Handbook shows you what your security controls are doing and how they are standing up to various inside and outside threats. This handbook provides guidance and techniques for evaluating and testing various computer security controls in IT systems. Author Leighton Johnson shows you how to take FISMA, NIST Guidance, and DOD actions and provide a detailed, hands-on guide to performing assessment events for information security professionals who work with US federal agencies. As of March 2014, all agencies are following the same guidelines under the NIST-based Risk Management Framework. This handbook uses the DOD Knowledge Service and the NIST Families assessment guides as the basis for needs assessment, requirements, and evaluation efforts for all of the security controls. Each of the controls can and should be evaluated in its own unique way, through testing, examination, and key personnel interviews. Each of these methods is discussed. Provides direction on how to use SP800-53A, SP800-115, DOD Knowledge Service, and the NIST Families assessment guides to implement thorough evaluation efforts for the security controls in your organization. Learn how to implement proper evaluation, testing, and assessment procedures and methodologies with step-by-step walkthroughs of all key concepts. Shows you how to implement assessment techniques for each type of control, provide evidence of assessment, and proper reporting techniques.